Domande frequenti sui messaggi di errore e di sistema del controller WLC

Sommario

Introduzione

Questo documento descrive le domande frequenti (FAQ) sui messaggi di errore e i messaggi di sistema per i Cisco Wireless LAN (WLAN) Controller (WLC).

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Domande frequenti sui messaggi di errore

D. È iniziata la conversione di oltre 200 access point (AP) da software Cisco IOS® a Lightweight AP Protocol (LWAPP) con un Cisco 4404 WLC. La conversione di 48 AP è stata completata e il messaggio ricevuto sul WLC afferma: `[ERRORE] spam_lrad.c 4212: impossibile unire l'access point perché è stato raggiunto il numero massimo di access point sull'interfaccia 1.` Perché si verifica l'errore?

R.È necessario creare interfacce AP-manager aggiuntive per supportare più di 48 access point. In caso contrario, viene visualizzato l'errore seguente:

```
Wed Sep 28 12:26:41 2005 [ERROR] spam_lrad.c 4212: AP cannot join because
the maximum number of APs on interface 1 is reached.
```

Configurare più interfacce AP-manager e configurare le porte primarie/di backup che altre interfacce AP-manager non utilizzano. Per visualizzare altri access point, è necessario creare una seconda interfaccia AP-manager. Verificare tuttavia che le configurazioni della porta principale e della porta di backup per ogni manager non si sovrappongano. In altre parole, se AP-manager 1 utilizza la porta 1 come porta primaria e la porta 2 come backup, AP-manager 2 deve utilizzare la porta 3 come porta primaria e la porta 4 come backup.

D. Dispongo di un controller WLC (Wireless LAN Controller) 4402 e utilizzo 1240 Lightweight Access Point (LAP). Ho abilitato la crittografia a 128 bit sul WLC. Quando si seleziona la crittografia WEP a 128 bit sul WLC, viene visualizzato un messaggio di errore che indica che la crittografia a 128 bit non è supportata sul modello 1240s: `[ERROR] spam_lrad.c 12839: Not creating SSID mode on CISCO AP xx:xx:xx:xx:xx:xx:xx perché il protocollo WEP a 128 bit non è supportato.` Perché viene visualizzato questo errore?

A.Le lunghezze delle chiavi mostrate sui WLC sono in realtà il numero di bit che sono nel segreto condiviso e non includono i 24 bit del vettore di inizializzazione (IV). Molti prodotti, tra cui Aironet, lo chiamano chiave WEP a 128 bit. In realtà è una chiave a 104 bit con IV a 24 bit. La dimensione della chiave pari a 104 bit è quella che deve essere abilitata sul WLC per la crittografia WEP a 128 bit.

Se si sceglie la dimensione della chiave a 128 bit sul WLC, si tratta in realtà di una crittografia della chiave WEP a 152 bit (128 + 24 IV). Solo i Cisco serie 1000 LAP (AP1010, AP1020, AP1030) supportano l'uso dell'impostazione della chiave WLC 128 bit WEP.

D. Perché la `dimensione della chiave WEP di 128 bit non è supportata sui modelli AP 11xx, 12xx e 13xx? Impossibile eseguire il push della WLAN in questi access point.` Messaggio di errore durante il tentativo di configurare WEP su un WLC?

R.Su un controller LAN wireless, quando si sceglie WEP statico come metodo di sicurezza di layer 2, sono disponibili queste opzioni per le dimensioni della chiave WEP.

- non impostato
- 40 bit
- 104 bit
- 128 bit

Questi valori delle dimensioni della chiave non includono il vettore di inizializzazione a 24 bit (IV), concatenato con la chiave WEP. Pertanto, per un WEP a 64 bit, è necessario scegliere **40** bit come dimensione della chiave WEP. Il controller aggiunge la versione IV a 24 bit per creare una chiave WEP a 64 bit. Analogamente, per una chiave WEP a 128 bit, scegliete **104 bit**.

I controller supportano anche chiavi WEP a 152 bit (128 bit + 24 bit IV). Questa configurazione non è supportata sui punti di accesso modello 11xx, 12xx e 13xx. Pertanto, quando si tenta di configurare WEP con 144 bit, il controller visualizza un messaggio per informare che la configurazione WEP non è stata trasferita ai punti di accesso di modello 11xx, 12xx e 13xx.

D. I client non sono in grado di eseguire l'autenticazione su una WLAN configurata per WPA2 e il controller visualizza il messaggio di errore `apf_80211.c:1923 APF-1-PROC_RSN_WARP_IE_FAILED: Unable to process the RSN and WARP IE station not using RSN (WPA2) on WLAN require RSN.MobileStation:00:0c:f1:0c:51:22, SSID:<>`. Perché viene visualizzato questo errore?

R.Questo problema è dovuto principalmente all'incompatibilità sul lato client. Per risolvere il problema, provare la seguente procedura:

- Verificare che il client sia certificato Wi-Fi per WPA2 e controllare la configurazione del client per WPA2.
- Controllare il data sheet per verificare se l'utility client supporta WPA2. Installare le patch rilasciate dal fornitore per supportare WPA2. Se si utilizza Utilità di Windows, assicurarsi di aver installato la patch WPA2 di Microsoft per supportare WPA2. Per ulteriori informazioni, vedere il supporto Microsoft.
- Aggiornare il driver e il firmware del client.
- Disattivare le estensioni Aironet sulla WLAN.

D. Una volta riavviato il WLC, ricevo il messaggio di errore `Mon Jul 17 15:23:28 2006 MFP Anomaly Detected - 3023 Invalid MIC events found as violated by the radio 00:XX:XX:XX:XX and detected by the dot11 interface at slot 0 of AP 00:XX:XX:XX:XX in 300 secondi quando osservo le risposte della sonda, beacon Frames.` Perché si verifica questo errore e come eliminarlo?

A. Questo messaggio di errore viene visualizzato quando i LAP abilitati per MFP rilevano frame con valori MIC non corretti. Per ulteriori informazioni sull'MFP, fare riferimento agli esempi di configurazione di Infrastructure Management Frame Protection (MFP) con WLC e LAP. Eseguire uno dei quattro passaggi seguenti:

1. Controllare e rimuovere tutti i punti di accesso o i client non validi nella rete che generano frame non validi.
2. Disabilitare la funzione PAP infrastruttura, se la funzione PAP non è abilitata sugli altri membri del gruppo di mobilità, in quanto i LAP possono ascoltare i frame di gestione dai LAP di altri WLC del gruppo per cui non è abilitata la funzione PAP. Per ulteriori informazioni sul gruppo di mobilità, fare riferimento alle domande frequenti sui gruppi di mobilità WLC (Wireless LAN Controller).
3. La correzione di questo messaggio di errore è disponibile nelle versioni WLC 4.2.12.0 e 5.0.148.2. Aggiornare i WLC a una di queste versioni.
4. Come ultima opzione, provare a ricaricare il LAP che genera questo messaggio di errore.

Q. Il client AIR-PI21AG-E-K9 si associa correttamente a un punto di accesso (AP) con autenticazione flessibile Extensible Authentication Protocol tramite Secure Tunneling (EAP-FAST). Tuttavia, quando l'access point associato è spento, il client non effettua il roaming verso un altro access point. Questo messaggio viene visualizzato continuamente nel log dei messaggi del controller: "Fri Jun 2 14:48:49 2006 [SECURITY] 1x_auth_pae.c 1922: Unable to allow user into the system - may the user is already login the system? Venerdì 2 giu 14:48:49 2006 [SECURITY] apf_ms.c 2557: Unable to delete username for mobile 00:40:96:ad:75:f4". Perché?

A.Quando la scheda client deve eseguire il roaming, invia una richiesta di autenticazione, ma non gestisce correttamente le chiavi (non informa il punto di accesso/controller, non risponde alla riautenticazione).

Questa condizione è documentata nel bug Cisco IDCSCsd02837. Questo bug è stato risolto con l'installazione guidata delle schede client Cisco Aironet 802.11a/b/g 3.5.

In generale, `l'errore Impossibile eliminare il nome utente per` mobilemessage si verifica anche per uno dei seguenti motivi:

- Il nome utente specifico viene utilizzato su più dispositivi client.
- Il metodo di autenticazione utilizzato per la WLAN ha un'identità anonima esterna. Ad esempio, in PEAP-GTC o in EAP-FAST, è possibile definire un nome utente generico come identità esterna (visibile) e il nome utente reale è nascosto all'interno del tunnel TLS tra il client e il server radius, quindi il controller non può visualizzarlo e utilizzarlo. In questi casi, il messaggio può essere visualizzato. Questo problema si verifica più comunemente con alcuni client firmware di terze parti e di vecchia generazione.

  Nota: solo gli utenti Cisco registrati possono accedere alle informazioni e agli strumenti dei bug Cisco interni.

D. Quando si installa il nuovo blade WiSM (Wireless Services Module) nello switch 6509 e si implementa il protocollo PEAP (Protected Extensible Authentication Protocol) con il server Microsoft IAS, viene visualizzato il seguente messaggio di errore: *Mar 1 00:00:23.526: %LWAPP-5-CHANGED: LWAPP ha cambiato stato in DISCOVERY *Mar 1 00:00:23.700: %SYS-5-RELOAD: richiesto da LWAPP CLIENT.Reload Motivo: FAILED CRYPTO INIT. *Mar 1 0:00:23.700: %LWAPP-5-CHANGED: LWAPP ha modificato lo stato in DOWN *Mar 1 00:00:23.528: %LWAPP-5-CHANGED: LWAPP ha modificato lo stato in DISCOVERY *Mar 1 00:00:23.557: LWAPP_CLIENT_ERROR_DEBUG:lwapp_crypto_init_ssc_keys_and_certs

no certs in SSC Private File *Mar 10:00:23.5 7: LWAPP_CLIENT_ERROR_DEBUG: *Mar 1 00:00:23.557: lwapp_crypto_init: errore di PKI_StartSession *Mar 1 00:00:23.706: %SYS-5-RELOAD: ricaricamento richiesto dal CLIENT LWAPP. . Perché?

I debug di A.RADIUS e dot1x mostrano che il WLC invia una richiesta di accesso, ma non è presente alcuna risposta dal server IAS. Per risolvere il problema, completare i seguenti passaggi:

1. Controllare e verificare la configurazione del server IAS.
2. Controllare il file di registro.
3. Installare software, ad esempio Etheral, che possa fornire i dettagli di autenticazione.
4. Arrestare e avviare il servizio IAS.

D. I Lightweight Access Point (LAP) non si registrano con il controller. Quale può essere il problema? Sul controller vengono visualizzati questi messaggi di errore: **Thu feb 3 03:20:47 2028: La richiesta di accesso LWAPP non include un certificato valido in CERTIFICATE_PAYLOAD da AP 00:0b:85:68:f4:f0. Thu feb 3 03:20:47 2028: Impossibile liberare la chiave pubblica per AP 00:0B:85:68:F4:F0.**

A. Quando il punto di accesso (AP) invia la richiesta di unione Lightweight Access Point Protocol (LWAPP) al WLC, incorpora il relativo certificato X.509 nel messaggio LWAPP. Viene inoltre generato un ID sessione casuale incluso nella richiesta di partecipazione LWAPP. Quando il WLC riceve la richiesta di aggiunta LWAPP, convalida la firma del certificato X.509 con la chiave pubblica degli access point e verifica che il certificato sia stato rilasciato da un'autorità di certificazione attendibile. Vengono inoltre analizzate la data e l'ora di inizio dell'intervallo di validità del certificato AP e la data e l'ora vengono confrontate con la data e l'ora corrispondenti.

Questo problema può essere causato da un'impostazione errata dell'orologio sul WLC. Per impostare l'orologio sul WLC, usare il comando show time e config time comandi.

D. Impossibile aggiungere un access point Lightweight Protocol (LWAPP) al controller. Nel log di Wireless LAN Controller (WLC) viene visualizzato un messaggio simile al seguente: **LWAPP Join-Request non include un certificato valido in CERTIFICATE_PAYLOAD restituito dal punto di accesso 00:0b:85:68:ab:01.** Perché?

A.È possibile ricevere questo messaggio di errore se il tunnel LWAPP tra l'access point e il WLC attraversa un percorso di rete con una MTU inferiore a 1500 byte. In questo modo, i pacchetti LWAPP vengono frammentati. Si tratta di un bug noto nel controller. Fare riferimento al bug Cisco IDCSCsd39911.

La soluzione è aggiornare il firmware del controller alla versione 4.0(155).

> **Nota**: solo gli utenti Cisco registrati possono accedere alle informazioni e agli strumenti dei bug Cisco interni.

D. Desidero stabilire un tunneling guest tra il controller interno e il controller di ancoraggio virtuale nella zona demilitarizzata (DMZ). Tuttavia, quando un utente tenta di associarsi a un SSID guest, non è in grado di ricevere l'indirizzo IP dalla DMZ, come previsto. Pertanto, il traffico utente non viene tunneling al controller sulla DMZ. L'output del comando debug mobile handoff visualizza un messaggio simile al seguente: **Security Policy Mismatch for WLAN <Wlan ID>. Richiesta di esportazione di ancoraggio dall'indirizzo IP dello switch: <indirizzo IP controller> ignorata.** Qual è il problema?

Il tunneling guest offre una maggiore sicurezza per l'accesso degli utenti guest alla rete wireless

aziendale. In questo modo gli utenti guest non possono accedere alla rete aziendale senza prima passare attraverso il firewall aziendale. Quando un utente si associa a una WLAN designata come WLAN guest, il traffico viene tunneling al controller WLAN che si trova sulla DMZ al di fuori del firewall aziendale.

Ora, considerando questo scenario, possono esserci diversi motivi per cui il tunneling guest non funziona come previsto. Come suggerisce l'output del comando debug, il problema può essere causato da una mancata corrispondenza in uno dei criteri di sicurezza configurati per quella particolare WLAN nel controller interno e nella DMZ. Verificare se i criteri di protezione e altre impostazioni, ad esempio le impostazioni di timeout della sessione, sono corrispondenti.

Un altro motivo comune è che il controller DMZ non è ancorato a se stesso per quella particolare WLAN. Per il corretto funzionamento del tunneling guest e per consentire alla DMZ di amministrare l'indirizzo IP dell'utente (utente che appartiene a una WLAN guest), è essenziale che venga eseguito il corretto ancoraggio per quella particolare WLAN.

D. Vedo molti messaggi `"CPU Receive Multicast Queue is full on Controller"` sul controller WLC del 2006, ma non sui WLC del 4400. Perché? Il multicast è stato disattivato sui controller. Qual è la differenza nel limite della coda multicast tra le piattaforme WLC 2006 e 4400?

A. Poiché il multicast è disabilitato sui controller, i messaggi che causano questo allarme possono essere messaggi ARP (Address Resolution Protocol). La profondità di coda (512 pacchetti) non differisce tra i 2000 WLC e i 4400 WLC. La differenza è che la NPU 4400 filtra i pacchetti ARP, mentre tutto viene eseguito nel software del 2006. Questo spiega perché il WLC del 2006 vede i messaggi ma non il WLC 4400. Un WLC 44xx elabora pacchetti multicast tramite hardware (tramite CPU). Un WLC 2000 elabora pacchetti multicast tramite software. L'elaborazione della CPU è più efficiente del software. Di conseguenza, la coda del 4400 viene cancellata più velocemente, mentre il WLC del 2006 fa fatica quando vede molti di questi messaggi.

D. Viene visualizzato il messaggio di errore `"[SECURITY] apf_foreignap.c 763: STA [00:0A:E4:36:1F:9B] Received a packet on port 1 but no Foreign AP configure for this port."` in uno dei controller. Che cosa significa questo errore e quali misure devo adottare per risolverlo?

A.Questo messaggio viene visualizzato quando il controller riceve una richiesta DHCP per un indirizzo MAC per cui non dispone di una macchina a stati. Questo è spesso visto da un bridge o da un sistema che esegue una macchina virtuale come VMWare. Il controller resta in ascolto delle richieste DHCP perché esegue lo snooping DHCP in modo da sapere quali indirizzi sono associati ai client collegati ai relativi punti di accesso (AP). Tutto il traffico per i client wireless passa attraverso il controller. Quando la destinazione di un pacchetto è un client wireless, il pacchetto va al controller e quindi passa attraverso il tunnel LWAPP (Lightweight Access Point Protocol) per il punto di accesso e lo spegne per il client. Per evitare che il messaggio venga visualizzato, è possibile consentire solo le VLAN usate sul controller sul trunk che va al controller con il comando **switchport vlan** allow sullo switch.

D. Perché viene visualizzato questo messaggio di errore sulla console: `Msg 'Set Default Gateway' of System Table failed, Id = 0x0050b986 error value = 0xffffffc`?

R. Ciò può essere dovuto a un elevato carico della CPU. Quando la CPU del controller è sovraccarica, ad esempio quando esegue copie di file o altre attività, non ha il tempo di elaborare tutti gli ACK inviati dalla NPU in risposta ai messaggi di configurazione. In questo caso, la CPU genera messaggi di errore. Tuttavia, i messaggi di errore non influiscono sul servizio o sulla funzionalità.

Per ulteriori informazioni, fare riferimento ai Cisco Wireless LAN Controller.

D. Sul mio sistema di controllo wireless (WCS) ricevo questi messaggi di errore relativi alla chiave WEP (Wired Equivalent Privacy): `la chiave WEP configurata sulla stazione può essere errata. L'indirizzo MAC della stazione è 'xx:xx:xx:xx:xx:xx', l'indirizzo MAC della radio base dell'access point è 'xx:xx:xx:xx:xx:xx' e l'ID dello slot è '1'`. Tuttavia, non utilizzo WEP come parametro di sicurezza nella rete. Uso solo Wi-Fi Protected Access (WPA). Perché si ricevono questi messaggi di errore WEP?

R.Se tutte le configurazioni sono perfette, i messaggi che ricevi al momento sono dovuti a bug. Il controller contiene alcuni bug noti. Fare riferimento ai bug Cisco IDCSCse17260 e Cisco, ma con ID CSCse1202, in cui si afferma che "la chiave WEP configurata sulla stazione può essere errata **rispettivamente con i client WPA e TKIP**". In realtà, l'ID bug Cisco **CSCse17260** è un duplicato dell'ID bug Cisco **CSCse11202**. La correzione per Cisco ma con ID **CSCse11202** è già disponibile con WLC release 3.2.171.5.

> **Nota**: le ultime versioni di WLC contengono una correzione per questi bug.

> **Nota**: solo gli utenti Cisco registrati possono accedere alle informazioni e agli strumenti interni del bug di Cisco.

D. Uso un server RADIUS esterno per autenticare i client wireless tramite il controller. Il controller invia regolarmente questo messaggio di errore: `nessun server radius risponde`. Perché vengono visualizzati questi messaggi di errore?

A.Quando una richiesta va dal WLC al server RADIUS, ogni pacchetto ha un numero di sequenza a cui il WLC si aspetta una risposta. In assenza di risposta, viene visualizzato un messaggio che `indica che il server radius non risponde`.

Il tempo predefinito per l'ascolto del WLC dal server RADIUS è di 2 secondi. Questo valore viene impostato dall'interfaccia utente del WLC **inSecurity > authentication-server**. Il valore massimo è 30 secondi. Pertanto, può essere utile impostare questo valore di timeout sul valore massimo per risolvere il problema.

A volte, i server RADIUS eseguono **'scartamenti invisibili'** del pacchetto di richiesta proveniente dal WLC. Il server RADIUS può rifiutare questi pacchetti a causa di una mancata corrispondenza del certificato e per diversi altri motivi. Azione valida eseguita dal server. Inoltre, in questi casi, il controller può contrassegnare il server RADIUS come server che non risponde

Per risolvere il problema degli scarti automatici, disabilitare **la** funzione di failover **aggressivo** nel WLC.

Se la funzione di failover **aggressivo** è abilitata nel WLC, il WLC è troppo aggressivo per contrassegnare il server AAA come server che non risponde. Tuttavia, non è possibile eseguire questa operazione perché il server AAA non può rispondere solo a quel determinato client (elimina automaticamente). Può essere una risposta ad altri client validi (con certificati validi). Tuttavia, il WLC può ancora contrassegnare il server AAA come non rispondente e non funzionante.

Per superare questo problema, disabilitare **la** funzione di failover **aggressivo**. Per eseguire questa operazione, usare **il comando config radius aggressive-failover** disable dalla CLI del controller. Se questa opzione è disabilitata, il controller eseguirà il failover sul server AAA successivo solo se

sono presenti 3 client consecutivi che non riescono a ricevere una risposta dal server RADIUS.

D. Diversi client non sono in grado di associarsi a un LWAPP e il controller registra il messaggio di errore `IAPP-3-MSGTAG015: iappSocketTask: iappRecvPkt restituito.` Perché questo accade?

R.Ciò è dovuto principalmente a un problema con le schede di rete Intel che supportano CCX v4, ma che eseguono una versione del bundle client precedente alla 10.5.1.0. Se si aggiorna il software alla versione 10.5.1.0 o successive, il problema viene risolto. Per ulteriori informazioni sul messaggio di errore, fare riferimento al bug Cisco IDCSCsi91347.

> **Nota**: solo gli utenti Cisco registrati possono accedere alle informazioni e agli strumenti interni del bug di Cisco.

D. Viene visualizzato questo messaggio di errore sul controller WLC (Wireless LAN Controller): `Raggiunto numero massimo di tentativi di richiesta di identità EAP (21) per STA 00:05:4e:42:ad:c5.` Perché?

A.Questo messaggio di errore viene visualizzato quando l'utente tenta di connettersi a una rete WLAN protetta EAP e non ha superato il numero preconfigurato di tentativi EAP. Quando l'autenticazione dell'utente non riesce, il controller esclude il client e quest'ultimo non può connettersi alla rete fino alla scadenza del timer di esclusione o finché non viene sostituito manualmente dall'amministratore.

L'esclusione rileva i tentativi di autenticazione eseguiti da un singolo dispositivo. Quando il dispositivo supera il numero massimo di errori, l'indirizzo MAC non può più essere associato.

Esclusione:

- Dopo 5 errori di autenticazione consecutivi per le autenticazioni condivise (è escluso il sesto tentativo)
- Dopo 5 errori di associazione consecutivi per l'autenticazione MAC (il sesto tentativo è escluso)
- Dopo 3 errori di autenticazione EAP/802.1X consecutivi (il quarto tentativo è escluso)
- Qualsiasi errore del server delle policy esterne (NAC)
- Qualsiasi istanza di duplicazione degli indirizzi IP
- Dopo 3 errori consecutivi di autenticazione Web (il quarto tentativo è escluso)

Èpossibile configurare il timer per l'esclusione di un client e l'esclusione può essere abilitata o disabilitata a livello di controller o di WLAN.

D. Viene visualizzato questo messaggio di errore sul controller WLC (Wireless LAN Controller): `sullo switch WLC viene generato un avviso di categoria con gravità 1 tramite lo switch WLC 10.0.16.5. Il messaggio di errore è Controller 10.0.16.5. I server RADIUS non rispondono alle richieste di autenticazione.` Qual è il problema?

A.Ciò può essere dovuto all'ID bug Cisco CSCsc05495. A causa di questo bug, il controller inserisce periodicamente una coppia AV non corretta (attributo 24, "stato") nei messaggi di richiesta di autenticazione che violano una richiesta RFP RADIUS e causano problemi ad alcuni server di autenticazione. Questo bug è risolto nella versione 3.2.179.6.

> **Nota**: solo gli utenti Cisco registrati possono accedere alle informazioni e agli strumenti interni del bug di Cisco.

D. Viene visualizzato il messaggio di errore Noise Profile in Monitor > 802.11b/g Radios. Voglio capire perché vedo questo messaggio di ERRORE?

A.Lo stato Noise Profile FAILED/PASSED è impostato dopo il risultato del test eseguito dal WLC e in confronto alla soglia impostata corrente. Per default, il valore Disturbo (Noise) è impostato su -70. Lo stato FAILED indica che il valore di soglia per quel particolare parametro o punto di accesso (AP) è stato superato. È possibile regolare i parametri nel profilo, ma si consiglia di modificare le impostazioni dopo aver compreso chiaramente il progetto della rete e come può influire sulle prestazioni della rete.

Le soglie di Radio Resource Management (RRM) PASSED/FAILED (SUPERATO/NON RIUSCITO) sono impostate globalmente per tutti gli access point sui **parametri globali 802.11a > Auto** RF e **802.11b/g >** pagine **Auto** RF. Le soglie RRM PASSED/FAILED sono impostate singolarmente per questo access point nella pagina **802.11 AP Interfaces > Performance** Profilepage.

D. Non è possibile impostare la porta 2 come porta di backup per l'interfaccia AP-manager. Il messaggio di errore restituito è `Impossibile impostare la configurazione della porta.` È possibile impostare la porta 2 come porta di backup per l'interfaccia di gestione. La porta attiva corrente per entrambe le interfacce è la porta 1. Perché?

A.Un AP-manager non dispone di una porta di backup. In precedenza era supportato nelle versioni precedenti. A partire dalla versione 4.0, la porta di backup per l'interfaccia AP-manager non è supportata. Di regola, un singolo AP-manager deve essere configurato su ciascuna porta (nessun backup). Se si utilizza il LAG (Link Aggregation), è disponibile un solo AP-manager.

L'interfaccia statica (o permanente) di AP-manager deve essere assegnata alla porta 1 del sistema di distribuzione e deve avere un indirizzo IP univoco. Impossibile eseguire il mapping a una porta di backup. Generalmente è configurato sulla stessa VLAN o subnet IP dell'interfaccia di gestione, ma non è un requisito.

D. Viene visualizzato questo messaggio di errore: `L'access point '00:0b:85:67:6b:b0' ha ricevuto un errore WPA MIC sul protocollo '1' dalla stazione '00:13:02:8d:f6:41'. Le contromisure sono state attivate e il traffico è stato sospeso per 60 secondi.` Perché?

A.Message Integrity Check (MIC) incorporato in Wi-Fi Protected Access (WPA) include un contatore di frame che impedisce un attacco man-in-the-middle. Questo errore indica che un utente della rete desidera riprodurre il messaggio inviato dal client originale oppure che il client è difettoso.

Se un client non supera ripetutamente il controllo MIC, il controller disabilita la WLAN sull'interfaccia AP in cui vengono rilevati gli errori per 60 secondi. Viene registrato il primo errore MIC e viene avviato un timer per consentire l'applicazione delle contromisure. Se si verifica un errore MIC successivo entro 60 secondi dall'errore precedente più recente, un STA la cui entità IEEE 802.1X ha agito come supplicant invaliderà se stesso o invaliderà tutti gli STA con un'associazione di sicurezza se la sua entità IEEE 802.1X ha agito come autenticatore.*

Inoltre, il dispositivo non riceve o trasmette frame di dati crittografati TKIP e non riceve o trasmette frame di dati non crittografati diversi dai messaggi IEEE 802.1X a o da alcun peer per un periodo di almeno 60 secondi dopo aver rilevato il secondo errore. Se il dispositivo è un punto di accesso, non saranno consentite nuove associazioni con TKIP durante questo periodo di 60 secondi; al termine del periodo di 60 secondi, l'punto di accesso riprenderà le normali operazioni e consentirà alle STA di (ri)associare.

In questo modo si evita un possibile attacco allo schema di crittografia. Questi errori MIC non possono essere disattivati nelle versioni WLC precedenti alla 4.1. Con Wireless LAN Controller versione 4.1 e successive, è disponibile un comando per modificare il tempo di scansione per gli errori MIC. Il comando **isconfig wlan security tkip tiene premuto <0-60 secondi> <id wlan>**. Usare il valore 0 per disabilitare il rilevamento degli errori MIC per le contromisure.

*Invalidare: terminare l'autenticazione.

D. Questo messaggio di errore viene visualizzato nei log del controller: `[ERRORE] dhcp_support.c 357: dhcp_bind(): servPort dhcpstate failed.` Perché?

A.Questi messaggi di errore vengono visualizzati principalmente quando la porta di servizio del controller ha DHCP abilitato, ma non riceve un indirizzo IP da un server DHCP.

Per impostazione predefinita, nell'interfaccia della porta del servizio fisico è installato un client DHCP e viene eseguita la ricerca di un indirizzo tramite DHCP. Il WLC tenta di richiedere un indirizzo DHCP per la porta del servizio. Se non è disponibile alcun server DHCP, la richiesta DHCP per la porta del servizio avrà esito negativo. Pertanto, in questo modo vengono generati i messaggi di errore.

Per ovviare al problema, è possibile configurare un indirizzo IP statico sulla porta di servizio (anche se la porta di servizio è disconnessa) oppure rendere disponibile un server DHCP per assegnare un indirizzo IP alla porta di servizio. Quindi, ricaricare il controller, se necessario.

La porta di servizio è in realtà riservata alla gestione fuori banda del controller e al ripristino del sistema, nonché alla manutenzione in caso di guasto della rete. Inoltre, è l'unica porta attiva quando il controller è in modalità di avvio. La porta di servizio non può contenere tag 802.1Q. Pertanto, deve essere collegata a una porta di accesso sullo switch adiacente. L'utilizzo della porta di servizio è facoltativo.

L'interfaccia della porta di servizio controlla le comunicazioni attraverso e viene mappata in modo statico dal sistema alla porta di servizio. Deve avere un indirizzo IP su una subnet diversa da gestione, AP-manager e da qualsiasi interfaccia dinamica. Inoltre, non può essere mappato a una porta di backup. La porta di servizio può utilizzare DHCP per ottenere un indirizzo IP oppure può essere assegnata a un indirizzo IP statico, ma non è possibile assegnare un gateway predefinito all'interfaccia della porta di servizio. Le route statiche possono essere definite tramite il controller per l'accesso remoto alla porta del servizio.

D. I client wireless non sono in grado di connettersi alla rete LAN wireless (WLAN). Il WiSM a cui è connesso il punto di accesso (AP) riporta questo messaggio: `Big NAV Dos attack from AP with Base Radio MAC 00:0g:23:05:7d:d0, Slot ID 0 and Source MAC 00:00:00:00:00:00.` Cosa significa questo?

A.Come condizione per accedere al supporto, il livello MAC controlla il valore del proprio vettore di allocazione di rete (NAV). Il NAV è un contatore residente in ogni stazione che rappresenta il tempo necessario al frame precedente per inviare il proprio frame. Il NAV deve essere zero prima che una stazione possa tentare di inviare un frame. Prima della trasmissione di un frame, una stazione calcola la quantità di tempo necessaria per inviare il frame in base alla lunghezza del frame e alla velocità dei dati. La stazione inserisce un valore che rappresenta questa ora nel campo della durata nell'intestazione del fotogramma. Quando le stazioni ricevono il frame, esaminano il valore del campo relativo alla durata e lo utilizzano come base per impostare i NAV corrispondenti. Questo processo riserva il supporto alla stazione di invio.

Un NAV alto indica la presenza di un valore NAV gonfiato (meccanismo di rilevamento della

portante virtuale per 802.11). Se l'indirizzo MAC segnalato è 00:00:00:00:00:00, è probabile che sia oggetto di spoofing (potenzialmente un attacco reale) ed è necessario confermarlo con l'acquisizione di un pacchetto.

D. Dopo aver configurato il controller e averlo riavviato, non è possibile accedervi in modalità https (Secure Web). Questo messaggio di errore viene visualizzato quando si tenta di accedere alla modalità Web protetta del controller: `Web protetto: Certificato di autenticazione Web non trovato (errore)`. Qual è la ragione di questo problema?

R.Questo problema può essere dovuto a diversi motivi. Un motivo comune può essere correlato alla configurazione dell'interfaccia virtuale del controller. Per risolvere il problema, rimuovere l'interfaccia virtuale e rigenerarla con questo comando:

```
WLC>config interface address virtual 1.1.1.1
```

Quindi, riavviare il controller. Dopo il riavvio del controller, generare nuovamente il certificato webauth localmente nel controller con questo comando:

```
WLC>config certificate generate webauth
```

Nell'output di questo comando è visualizzato il messaggio:`È stato generato il certificato di autenticazione Web.`

Èora possibile accedere alla modalità Web protetta del controller al riavvio.

D. A volte i controller segnalano questo messaggio di avviso di attacco di tipo firma di allagamento di disassociazione IDS contro client validi in cui l'indirizzo MAC dell'autore dell'attacco è quello di un punto di accesso (AP) aggiunto al controller. `Avviso: attacco di tipo firma di tipo 'Disassoc flood' di IDS rilevato sul punto di accesso '<nome AP>', protocollo '802.11b/g', controller 'x.x.x'. La descrizione della firma è 'Flood dissociazione', con la precedenza 'x'. L'indirizzo MAC dell'autore dell'attacco è 'hh:hh:hh:hh:hh', il numero di canale è 'x' e il numero di rilevamenti è 'x'`. Perché questo accade?

A.Questo problema è causato dal bug Cisco IDCSCsg81953 .

> **Nota**: solo gli utenti Cisco registrati possono accedere alle informazioni e agli strumenti interni del bug di Cisco.

Disassociazione IDS Gli attacchi Flood contro client validi vengono talvolta segnalati quando l'indirizzo MAC dell'autore dell'attacco è quello di un access point collegato a quel controller.

Quando un client è associato all'access point ma interrompe le comunicazioni a causa della rimozione della scheda, rimane fuori dall'intervallo e così via per raggiungere l'access point, che attende il timeout di inattività. Una volta raggiunto il timeout di inattività, l'access point invia al client un frame non associato. Quando il client non riconosce il frame non associato, l'access point trasmette nuovamente il frame più volte (circa 60 frame). Il sottosistema IDS del controller ascolta questi ritrasmissioni e avvisi con questo messaggio.

Il bug è stato risolto nella versione 4.0.217.0. Aggiornare la versione del controller a questa versione per risolvere il problema relativo a questo messaggio di avviso per i client e gli access

point validi.

D. Nel syslog del controller viene visualizzato il seguente messaggio di errore: **[WARNING] apf_80211.c_2408: Received a message with a invalid supported rate from station <xx:xx:xx:xx:xx:xx> [ERROR] apf_utils.c 198: Missing Supported Rate.** Perché?

A. In realtà, i messaggi `Missing Supported Rate (Frequenza supportata mancante)` indicano che il WLC è configurato per alcune velocità dati richieste secondo le impostazioni wireless, ma la scheda NIC non ha la velocità richiesta.

Se sul controller sono impostate velocità dati, ad esempio 1 e 2 MB, ma la scheda NIC non comunica su tali velocità dati, è possibile ricevere questo tipo di messaggio. Si tratta di un comportamento errato della scheda NIC. D'altro canto, se il controller è 802.11g abilitato e il client è una scheda 802.11b(only), si tratta di un messaggio legittimo. Se questi messaggi non causano problemi e le schede possono ancora connettersi, questi messaggi possono essere ignorati. Se i messaggi sono specifici della scheda, verificare che il driver per la scheda sia aggiornato.

D. Questo syslog **AP:001f.ca26.bfb4: %LWAPP-3-CLIENTERRORLOG: Decodifica messaggio: impossibile trovare corrispondenza con ID WLAN <id>** messaggio di errore trasmesso sulla rete. Perché questo accade e come lo fermo?

A. Questo messaggio viene trasmesso dai LAP. Questa condizione viene rilevata quando si configura la funzione di override della WLAN per una WLAN e la WLAN in questione non viene annunciata.

`Configurare l'access point syslog host global 0.0.0.0` per arrestarlo oppure inserire un indirizzo IP specifico se si dispone di un server syslog in modo che il messaggio venga trasmesso solo al server.

D. Viene visualizzato questo messaggio di errore sul controller WLC: **[ERROR] File: apf_mm.c : Line: 581 : Announce collision for mobile 00:90:7a:05:56:8a, deleteting.** Perché?

R.In genere, questo messaggio di errore indica che il controller ha annunciato collisioni per un client wireless (ovvero, i diversi access point annunciano di avere il client) e il controller non ha ricevuto un handoff da un access point al successivo. Nessuno stato di rete da mantenere. Eliminare il client wireless e chiedere al client di riprovare. Se il problema si verifica di frequente, potrebbe trattarsi di un problema relativo alla configurazione della mobilità. In caso contrario, può trattarsi di un'anomalia correlata a un client o a una condizione specifici.

D. Il mio controller lancia questo messaggio di allarme: **La soglia di copertura di '12' è stata violata.** Che cos'è questo errore e come risolverlo?

A.Questo messaggio di allarme viene generato quando il rapporto segnale-rumore (SNR, Signal-to-Noise Ratio) di un client scende su un valore inferiore al valore di soglia SNR per la radio in questione. 12 è il valore di soglia SNR predefinito per il rilevamento dei fori di copertura.

L'algoritmo di rilevamento e correzione dei fori di copertura determina se esiste un foro di copertura quando i livelli SNR dei client sono inferiori a una determinata soglia SNR. Questa soglia SNR varia in base a due valori: la potenza di trasmissione del punto di accesso e il valore del profilo di copertura del controller.

In dettaglio, la soglia SNR del client è definita dalla potenza di trasmissione di ciascun punto di accesso (rappresentata in dBm), meno il valore costante di 17dBm, meno il valore configurabile

dall'utente del profilo di copertura (questo valore è predefinito a 12dB).

- **Valore limite SNR client (|dB|) = [Potenza di trasmissione AP (dBm) - Costante (17 dBm) - Profilo copertura (dB)]**

Èpossibile accedere al valore del profilo di copertura configurabile dall'utente nel modo seguente:

1. Nell'interfaccia utente del WLC, andare all'intestazione principale di Wireless e selezionare l'opzione **Network** (Rete) per lo standard WLAN desiderato sul lato sinistro (802.11a o 802.11b/g). Quindi, selezionare **Auto RF** nell'angolo superiore destro della finestra.
2. Nella pagina Parametri globali RF automatici individuare la sezione Soglie profilo. In questa sezione è possibile trovare il valore Copertura (da 3 a 50 dbm). Questo valore è il valore del profilo di copertura configurabile dall'utente.
3. Questo valore può essere modificato per influenzare il valore di soglia SNR del client. L'altro modo per influenzare questa soglia SNR è aumentare la potenza di trasmissione e compensare il rilevamento del buco di copertura.

D. Uso ACS v 4.1 e un controller WLC (Wireless LAN Controller) 4402. Quando il WLC tenta di autenticare un client wireless ad ACS 4.1, il WLC non risponde con l'ACS e segnala questo messaggio di errore: " *Si è verificato un errore interno* ". Tutte le configurazioni sono corrette. Perché si verifica questo errore interno?

R.C'è un bug Cisco relativo all'autenticazione IDCSCsh62641 nell'ACS 4.1, dove l'ACS restituisce `il` messaggio di `errore interno con` errore.

Questo bug può essere il problema. Per questo bug è disponibile una patch sul sito Download di ACS 4.1 che può risolvere il problema.

> **Nota**: solo gli utenti Cisco registrati possono accedere alle informazioni e agli strumenti interni del bug di Cisco.

D. Impossibile avviare Cisco serie 4400 Wireless LAN Controller (WLC). Questo messaggio di errore viene ricevuto sul controller: `** Impossibile utilizzare IDE 0:4 per il caricamento a freddo ** Errore (nessun IRQ) dev 0 blk 0: stato 0x51 Errore reg: 10 ** Impossibile leggere dal dispositivo 0.` Perché?

R.La causa di questo errore può essere un problema hardware. Apri una richiesta TAC per risolvere ulteriormente il problema. Per aprire una richiesta TAC, è necessario avere un contratto valido con Cisco. Per contattare Cisco TAC, consultare il supporto tecnico.

D. Il controller WLC (Wireless LAN Controller) si installa in problemi del buffer di memoria. Una volta che i buffer di memoria sono pieni, il controller si blocca e deve essere riavviato per riportarlo online. Questi messaggi di errore vengono visualizzati nel log dei messaggi: `Mon Apr 9 10:41:03 2007 [ERROR] dtl_net.c 506: Out of System buffer Mon Apr 9 10:41:03 2007 [ERROR] sysapi_if_net.c 537: Unable allocate new Mbuf. lun apr 9 10:41:03 2007 [ERROR] sysapi_if_net.c 219: MbufGet: no free Mbufs.` Perché?

A.Questo problema è dovuto al bug Cisco IDCSCsh93980. Il bug è stato risolto nella versione WLC 4.1.185.0. Per risolvere il problema, aggiornare il controller alla versione software o successiva.

> **Nota**: solo gli utenti Cisco registrati possono accedere alle informazioni e agli strumenti

interni del bug di Cisco.

D. Ho eseguito l'aggiornamento del controller WLC (Wireless LAN Controller) 4400 al codice 4.1 e il syslog è stato bombardato da messaggi come questo: May03 `03:55:49.591 dtl_net.c:1191 DTL-1-ARP_POISON_DETECTED: STA [00:17:f2:43:26:93, 0.0.0.0] ARP (op. 1) ricevuto con SPA 192.168.1.233/TPA 192.168.1.233 non valida`. Cosa indicano questi messaggi?

A. Questa condizione può verificarsi quando il protocollo WLAN è contrassegnato come DHCP richiesto. In questi casi, solo le stazioni che ricevono un indirizzo IP tramite DHCP possono essere associate. I client statici non possono essere associati a questa WLAN. WLC opera come agente di inoltro DHCP e registra l'indirizzo IP di tutte le stazioni. Questo messaggio di errore viene generato quando WLC riceve una richiesta ARP da una stazione prima di aver ricevuto i pacchetti DHCP dalla stazione e registrato il relativo indirizzo IP.

D. Quando si utilizza Power over Ethernet (PoE) sul controller LAN wireless Cisco 2106, le radio AP non sono abilitate. L'`access point non è in grado di verificare una quantità sufficiente di alimentazione in linea. Slot radio disabilitato.` viene visualizzato un messaggio di errore. Come posso risolvere il problema?

A.Questo messaggio di errore viene visualizzato quando lo switch, che accende il punto di accesso, è uno switch pre-standard ma l'access point non supporta la modalità di alimentazione di input pre-standard.

Uno switch Cisco pre-standard non supporta la gestione intelligente dell'alimentazione (IPM, Intelligent Power Management), ma ha alimentazione sufficiente per un punto di accesso standard.

Ènecessario attivare la modalità di alimentazione pre-standard sull'access point che viene segnalato da questo messaggio di errore. Questa operazione può essere eseguita dalla CLI del controller con l'opzione config ap power pre-standard {enable | disabilita} {all | Cisco_AP}.

Se necessario, questo comando deve essere già configurato se si esegue l'aggiornamento alla versione software 4.1 da una versione precedente. Tuttavia, è possibile che sia necessario immettere questo comando per le nuove installazioni o se si ripristinano i valori predefiniti dell'access point.

Sono disponibili i seguenti switch Cisco da 15 watt standard:

- AIR-WLC2106-K9
- WS-C350, WS-C3560, WS-C3750
- C1880
- 2600, 2610, 2611, 2621, 2650, 2651
- 2610XM, 2611XM, 2621XM, 2650XM, 2651XM, 2691
- 2811, 2821, 2851
- 3631-telco, 3620, 3640, 3660
- 3725, 3745
- 3825, 3845

D. Il controller genera un `dtl_arp.c:2003 DTL-3-NPUARP_ADD_FAILED: impossibile aggiungere una voce ARP per xx:xx.-xxx.x al processore di rete. La voce non esiste.` Messaggio syslog simile a questo. Qual è il significato di questo messaggio syslog?

R. Mentre alcuni client wireless inviano una risposta ARP, l'unità del processore di rete (NPU) deve conoscere tale risposta. Quindi, la risposta ARP viene inoltrata alla NPU, ma il software WLC non deve cercare di aggiungere questa voce al processore di rete. In tal caso, vengono generati questi messaggi. Ciò non comporta alcun impatto sulla funzionalità del WLC, ma questo messaggio di syslog viene generato dal WLC.

D. Ho installato e configurato un nuovo Cisco 2106 WLC. Il WLC indica che si è verificato un errore nel sensore della temperatura. Quando si accede all'interfaccia Web in "riepilogo controller", viene visualizzato "`errore sensore`" accanto alla temperatura interna. Tutto il resto sembra funzionare normalmente.

A.Il guasto del sensore di temperatura interno è di natura estetica e può essere risolto aggiornando il WLC alla versione 4.2.61.0.

WLC 2106 e WLC 526 **costruiti dopo il 07/01/2007** possono utilizzare il chip del sensore di temperatura di un altro fornitore. Questo nuovo sensore funziona correttamente ma non è compatibile con il software successivo alla versione 4.2. Pertanto, il software meno recente non è in grado di leggere la temperatura e visualizza questo errore. Tutte le altre funzionalità del controller non sono interessate da questo difetto.

Esiste un bug Cisco noto relativo a questo problema, IDCSCsk97299. Questo bug è menzionato nella nota sulla versione del WLC versione 4.2.

> **Nota**: solo gli utenti Cisco registrati possono accedere alle informazioni e agli strumenti interni del bug di Cisco.

D. Viene visualizzato il messaggio `radius_db.c:1823 AAA-5-RADSERVER_NOT_FOUND: Unable not find appropriate RADIUS server for WLAN <ID WLAN> - Unable to find a default server" (Impossibile trovare un server predefinito)` per TUTTI gli SSID. Questo messaggio viene visualizzato anche per gli SSID che non utilizzano server AAA.

A.Questo messaggio di errore indica che il controller non è stato in grado di contattare il server RADIUS predefinito o che non è stato definito alcun server RADIUS.

Una possibile causa di questo comportamento è il bug Cisco IDCSCsk08181, risolto nella versione 4.2. Aggiornare il controller alla versione 4.2.

D. Il `messaggio: lug 10 17:55:00.725 sim.c:1061 SIM-3-MACADDR_GET_FAIL: Impossibile trovare l'indirizzo MAC di origine dell'interfaccia 1.` Viene visualizzato un messaggio di errore sul controller WLC. Cosa indica questo?

A.Ciò significa che il controller ha riscontrato un errore durante l'invio di un pacchetto con origine CPU.

D. Questi messaggi di errore vengono visualizzati sul controller WLC:

- `Lug 10 14:52:21.902 nvstore.c:304 SYSTEM-3-FILE_READ_FAIL: impossibile leggere il file di configurazione 'cliWebInitParms.cfg'`
- `Lug 10 14:52:21.624 nvstore.c:304 SYSTEM-3-FILE_READ_FAIL: impossibile leggere il file di configurazione 'rfidInitParms.cfg'`
- `Lug 10 14:52:21.610 nvstore.c:304 SYSTEM-3-FILE_READ_FAIL: impossibile leggere il file di configurazione 'dhcpParms.cfg'`
- `Lug 10 14:52:21.287 nvstore.c:304 SYSTEM-3-FILE_READ_FAIL: impossibile leggere il file di`

configurazione 'bcastInitParms.cfg'

- Mar 18 16:05:56.753 osapi_file.c:274 OSAPI-5-FILE_DEL_FAILED: impossibile eliminare il file: sshpmInitParms.cfg. rimozione del file non riuscita. -Process: Nome:fp_main_task, Id:11ca7618
- Mar 18 16:05:56.753 osapi_file.c:274 OSAPI-5-FILE_DEL_FAILED: impossibile eliminare il file : bcastInitParms.cfg. rimozione del file non riuscita. -Process: Nome:fp_main_task, Id:11ca7618

D. Cosa indicano questi messaggi di errore?

A.Questi messaggi sono messaggi informativi e fanno parte della normale procedura di avvio. Questi messaggi vengono visualizzati a causa di un errore di lettura o eliminazione di diversi file di configurazione. Quando non vengono trovati file di configurazione particolari o se il file di configurazione non può essere letto, la sequenza di configurazione per ogni processo invia questo messaggio, ad esempio nessuna configurazione del server DHCP, nessuna configurazione di tag (ID RF) e così via. Si tratta di messaggi di bassa gravità che possono essere ignorati senza problemi. Questi messaggi non interrompono il funzionamento del controller.

Q. **HE6-WLC01,local0,alert,2008-07-25,12:48:18,apf_rogue.c:740 APF-1-UNABLE_TO_KEEP_ROUGE_CONTAINS: Unable to keep rogue 00:14:XX:02:XX:XX in contains state - no available AP to contains.** viene visualizzato un messaggio di errore. Cosa indica questo?

A.Ciò significa che l'access point che ha eseguito la funzione di contenimento rogue non è più disponibile e il controller non riesce a trovare alcun access point adatto per eseguire il contenimento rogue.

D. Il messaggio di sistema **DTL-1-ARP_POISON_DETECTED: STA [00:01:02:0e:54:c4, 0.0.0.0] ARP (op. 1) ricevuto con SPA 192.168.1.152/TPA 192.168.0.206 non valido** viene visualizzato sul controller LAN wireless. Cosa implica questo messaggio?

A. È possibile che il sistema abbia rilevato uno spoofing o un avvelenamento ARP. Tuttavia, questo messaggio non implica necessariamente che si sia verificato uno spoofing ARP dannoso. Il messaggio viene visualizzato quando si verificano le seguenti condizioni:

- Una WLAN è configurata con DHCP obbligatorio e un dispositivo client, dopo essersi associato a tale WLAN, trasmette un messaggio ARP senza prima completare il protocollo DHCP. Questo può essere un comportamento normale; può verificarsi, ad esempio, quando il client è indirizzato in modo statico o quando il client detiene un lease DHCP valido da un'associazione precedente. Il messaggio di errore può essere simile al seguente:

```
DTL-1-ARP_POISON_DETECTED: STA [00:01:02:0e:54:c4, 0.0.0.0] ARP (op 1) received with invalid SPA
192.168.1.152/TPA 192.168.0.206
```

Di conseguenza, il client non è in grado di inviare o ricevere alcun traffico di dati finché non esegue il DHCP tramite il WLC.

Per ulteriori informazioni, consultare la sezione Messaggi DTL della guida ai messaggi del sistema Cisco Wireless LAN Controller.

D. I LAP non utilizzano il sistema Power over Ethernet (POE) per l'accensione. Vengono visualizzati i registri sul controller LAN wireless:

AP's Interface:1(802.11a) Operation State Down: Base Radio MAC:XX:1X:XX:AA:VV:CD Cause=Low in-

line power

D. Qual è il problema?

R. Questo problema può verificarsi se le impostazioni di Power over Ethernet (POE) non sono configurate correttamente. Quando un punto di accesso che è stato convertito in modalità Lightweight, ad esempio, un AP1131 o AP1242 o un punto di accesso serie 1250 è alimentato da un alimentatore collegato a uno switch Cisco Pre-Intelligent Power Management (pre-IPM), è necessario configurare Power over Ethernet (PoE), noto anche come alimentazione in linea.

per ulteriori informazioni, fare riferimento a Configurazione del supporto Power over Ethernet ed Ethernet.

D. Viene visualizzato questo messaggio sul controller WLC:

```
*Mar 05 10:45:21.778: %LWAPP-3-DISC_MAX_AP2: capwap_ac_sm.c:1924 Dropping primary discovery
request from
AP XX:1X:XX:AA:VV:CD - maximum APs joined 6/6
```

D. Cosa indica ciò?

A.Lightweight Access Point traccia un determinato algoritmo per trovare un controller. Il processo di rilevamento e collegamento è descritto in dettaglio nella registrazione di un Lightweight AP (LAP) su un Wireless LAN Controller (WLC).

Questo messaggio di errore viene visualizzato sul WLC, quando riceve una richiesta di individuazione dopo aver raggiunto la capacità massima dell'AP.

Se il controller primario di un LAP non è configurato o è un nuovo LAP preconfigurato, invia richieste di rilevamento LWAPP a tutti i controller raggiungibili. Se le richieste di rilevamento raggiungono un controller in esecuzione alla capacità massima dell'access point, il WLC ottiene le richieste e si rende conto che si trova alla capacità massima dell'access point e non risponde alla richiesta e restituisce questo errore.

D. Dove posso trovare ulteriori informazioni sui messaggi di sistema LWAPP?

A. Per ulteriori informazioni sui messaggi di sistema LWAPP, consultare la Cisco Wireless LAN Controller System Message Guide, 4.2 (Ritirato).

D. Il messaggio di errore `Error extraction webauth files` (`Errore durante l'estrazione dei file webauth`) viene visualizzato sul controller WLC (Wireless LAN Controller). Cosa indica questo?

A.WLC non riesce a caricare un bundle Custom Web Authentication/Passthrough se uno dei file inclusi nel bundle ha più di 30 caratteri nel nome del file, che include l'estensione del file. Il pacchetto di autenticazione Web personalizzato prevede un limite massimo di 30 caratteri per i nomi di file. Assicuratevi che i nomi di file all'interno del fascio non siano più lunghi di 30 caratteri.

D. Controller LAN wireless (WLC), con codice 5.2 o 6.0 e un numero elevato di gruppi di punti di accesso, l'interfaccia utente Web non visualizza tutti i gruppi di punti di accesso configurati. Qual è il problema?

A.I gruppi di access point mancanti possono essere visualizzati se si usa la CLI **show wlan ap-groups**

Provare ad aggiungere un altro gruppo di punti di accesso all'elenco. Ad esempio, sono stati distribuiti 51 gruppi di access point e il 51° non è presente (pagina 3). Aggiungere il 52º gruppo e la pagina 3 deve essere visualizzata nell'interfaccia utente del Web.

Per risolvere il problema, eseguire l'aggiornamento alla versione WLC 7.0.220.0.

Informazioni correlate

- Domande frequenti sulla risoluzione dei problemi di WiSM
- Pagina di supporto wireless
- Supporto tecnico e download Cisco

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).